INFORMATION TECHNOLOGY AND WORKERS' PRIVACY: REGULATORY TECHNIQUES

Christophe Vigneau†

I. A QUESTION OF BALANCE

The introduction of new computer technologies at work has greatly modified the relationship between employers and employees. Two main effects of these technologies may be identified. The first is that they blur the frontiers between professional life and personal life. On the one hand, employees may, through computer technologies, have personal, even very private, time at work: employees who use the Internet for work may easily and smoothly move from a professional website to a website unrelated to their work. So, with one click of the mouse, an employee may pass from a work activity to a private one. But, on the other hand, the very same technologies make it possible for work to invade the employee's home. Official working hours do not mean anything when you can take your work home and carry on with it there, without any time limits.[1] The second main effect of the introduction of new computer technologies at work is that it increases the possibilities that employers have to monitor their employees' electronic communications. "Cyber-surveillance" is the most effective and intensive means of monitoring employees at work. The same computer technologies also make it easy for employers to collect and process information about their employees.

Because of all this, it must be expected that the introduction of new technologies at the workplace will create new legal problems and new challenges for lawyers. Many commentators seem to think that the law does not yet provide adequate tools to deal with these issues and that the development of adequate responses requires the

† Maître de Conférences de droit privé University of Paris I, (Panthéon-Sorbonne), France.

1. In a recent case, the highest court in France held that a worker has a right to refuse to have his office installed at home.

enactment of new laws. As is often the case nowadays, legislators are called upon to intervene and to fill what seems to be a gap in the law; thus there have been calls for the creation of new legal instruments that will regulate computer surveillance at work and the processing of personal data by employers. Nonetheless, we should still ask to what extent computer technologies really do pose new legal problems that require new legal solutions. The widespread introduction of computer technologies at workplaces certainly gives new urgency to the problems related to the protection of employees' rights to privacy; but, although the new circumstances may lead to new extremes, one may still ask whether these new technologies actually require changes in the way that lawyers address the protection of the right to privacy at work, and indeed whether new legislation is needed in this area.

The key question here is whether the introduction of information technologies into the workplace has changed the fundamental nature and terms of the debates about surveillance at work and about the processing of personal data about workers. The first of these issues, surveillance, requires a balance to be set between two opposing rights: on the one hand, the right of employers to check on the work that is being done for them by their employees and, on the other, the right of the employees to some degree of privacy. This balance is clearly set out in Article 20.3 of the Workers' Statute in Spain, according to which the employer may:

> . . .adopt the measures of surveillance and control that he sees fit in order to ensure that workers fulfil their contractual obligations and duties, paying due respect in the adoption and implementation of such measures to the human dignity of the workers. . . .

The terms of the legal debate are clearly presented here: Employers have a right to monitor their employees, but the employees have a right to have their human dignity respected—and thus, we may assume, to enjoy at least some degree of privacy. The second of the issues, the processing of personal data, is subject to a similar dichotomy: with the rights of employers to collect and process information about their employees (which derives from their right to run their businesses) standing against the rights of the employees to have their private lives respected.

In both cases, the employers' rights will affect the scope of the individual worker's right to privacy, a right which is widely recognized as one of the most basic of all individual rights. To start with, the *Universal Declaration of Human Rights* (1948), Article 12, states that: "no one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and

reputation. Everyone has the right to the protection of the law against such interference or attacks." The right to privacy is also established by Article 7 of the *European Charter of Fundamental Rights* and by Article 8 of the *European Convention on Human Rights*. Similar rights exist in many countries, at a high level within the hierarchy of legal norms. In the United States, the right to privacy is set out in the Fourth Amendment to the Constitution; and, in Brazil, Germany, Italy, and Spain, privacy rights have also been given constitutional status. In France, Article 9 of the Civil Law Code establishes that "everyone has a right to privacy." And even in the United Kingdom, which for a long time had no such laws, the *Human Rights Act 1998* applies the *European Convention on Human Rights*—which includes the right to have one's private life respected—to all aspects of national law.

Within the context of our comparative study of the law on workplace surveillance and the processing of workers' personal data, this paper examines the way in which different regulatory techniques are used in the attempt to reconcile these important rights to privacy with the rights enjoyed by employers. It will look at two different types of techniques: the first involves the establishment of a set of general principles and criteria that judges may then apply to individual cases (Section II); and the second involves the establishment of procedural rules that condition the way in which these rights may be exercised (Section III).

II. THE ESTABLISHMENT OF GENERAL PRINCIPLES

The national studies in this collection of papers show that certain concepts tend to be used in order to set the balance between the rights of employers and employees; judges use these concepts to help them interpret the facts and reach their decisions in individual cases. In that sense, these concepts are elevated to the level of legal principles. Two such concepts are of special and growing interest in matters related to surveillance at work and the processing of workers' personal data: relevance and proportionality. Both are useful tools in reconciling conflicting interests in general, but they are particularly important in this area of law, as they are very well adapted to dealing both with restrictions upon the exercise of powers (such as the limitation of the powers of employers implied by the application of employees' privacy rights) and with restrictions upon the exercise of fundamental rights (such as the limitations on the right to privacy which may result from exercise of the employers' rights to run their businesses). It therefore

appears appropriate and logical to use these concepts when considering privacy within the employment relation.

A. Relevance

The concept of relevance is teleological in that it requires all actions to have a specific (and lawful) goal against which they may be measured. It is a concept that appears in Article 18 of the *European Convention on Human Rights*, which states that, "the restrictions permitted under this Convention to the said rights and freedoms shall not be applied for any purpose other than those for which they have been prescribed." A principle of relevance is thus clearly established as regards the specific aims of any restrictions to the rights established by the Convention.

For the purposes of our present discussion, the grounds for restricting the employees' right to privacy is the right or need of employers to monitor the work done by their employees and the right or need to process personal data about them. So, applying a test for relevance, any actions taken in this respect by employers should have the clear aim of achieving this particular objective; that is, they must be related to a lawful aim of a professional nature. Monitoring and data processing must be related to the job which is done by each of the individual workers concerned or, at the very least, to the way in which the company is organized. The concept of relevance thus becomes a regulatory principle inasmuch as it requires the employer to justify each specific case of monitoring and data processing; any actions which have a purpose that is not employment-related are not relevant and thus unlawful. So, for example, any surveillance carried out away from the workplace or at a time when the employee is not on duty may be considered irrelevant and unlawful. Hence the decisions in some legal systems that cameras and microphones may not be installed in toilets or canteens; it is assumed that such surveillance is simply not relevant to the aim of checking on how employees do their job. There may be circumstances in which this assumption may be overturned—where, for example, there are grounds for suspicion that employees are committing serious offenses in these places—but it would be for an employer to show this and thus to prove the relevance of a particular action in a particular case. (Everything will depend on the facts of the particular case; a camera in a canteen might be relevant for dealing with concerns over time-wasting, in that it could show how long each employee spends on his or her break; but a microphone installed alongside the camera might

produce a lot of information that would not be relevant for this purpose and so be unlawful.)

Similar considerations may apply to the monitoring of private e-mails sent and received by employees, as is clear from the *Nikon* case, where the highest court in France held that it was unlawful for the employer to open an employee's private e-mail even though the company's policy established a clear prohibition on the private use of the computer facilities. Relying on the principle of relevance, the Court held that an employer may only examine the contents of an employee's computer when it is clear that these contents are of a professional nature: when contents that are clearly of a private nature are found, this is a sufficient basis for taking disciplinary action for the breach of any prohibition on private use. But to go on to examine the contents of a private message does not serve any aim related to the control of the employee's working activities, and so it was held to be irrelevant to any legitimate aim that the employer might have, and therefore unlawful.[2]

Some national legislation even establishes a general requirement that limitations upon the rights of workers be relevant to their stated purpose. For example, Article L.120-2 of the French Labour Code states that employers may "not place restrictions on the rights of persons or on their individual or collective liberties unless these are justified by the nature of the work and are proportional to the goal sought." This Article clearly requires that any workplace surveillance or processing of personal data (both of which may restrict the workers' rights to privacy) be relevant to the aim of checking on their working activities.

The same requirement of relevance restricts the scope that employers throughout the European Union have to collect personal data about their employees. Under Article 6(1)(c) of Directive 95/46/EC, all processing of personal data must be "adequate, relevant and not excessive in relation to the purposes for which they were collected and/or further processed." Because the focus of the Directive is the processing of personal data in general (and not just within the employment relationship), the purposes against which relevance must be tested may appear to be much more related to the general aims and functioning of the employers' organization, than to matters of employment; but, in practice, any test of relevance with respect to the processing of personal data about workers will depend

2. For a longer discussion of this case, *see* Christophe Vigneau, *Information Technology and Workers' Privacy: The French Law*, 23 COMP LAB. L & POL'Y J. 351 (2002).

to a large extent on the nature of the work done by those workers. To take some examples: First, an employer may lawfully process certain personal data about employees as part of the creation of a company "yearbook" (a document whose very purpose is to present the employees of the company to others, within or outside that company). However, this does not mean that employers may put any personal data they choose in such a publication; some data are clearly irrelevant to the purposes of a "yearbook" that it would be unlawful for these to be processed. The question is then to define the range of (lawful) purposes which a "yearbook" may serve and to prohibit any data processing which is not relevant to any of these aims. A second example is the processing of personal data by ideologically-based organizations, such as churches and religious schools. In this case, the processing of certain sensitive personal data about workers (such as their religious beliefs and family situation) might be considered relevant for the purposes of those organizations. And a third example is the application of the principle of relevance during the process of recruitment. In some countries, there is a specific legal requirement that all the information asked of a candidate should only relate to the assessment of his or her capacity to do the job in question. The difficulty here is, of course, that employers may claim that a wide range of personal data are relevant in making just such an assessment. Possibly for this reason, legislation in most countries identifies a series of factors which are clearly not relevant; for example, by expressly forbidding employers to take into account the sex, race, age, or pregnancy of a candidate.

Such specific regulations are, however, the exception rather than the rule. In general, the concept of relevance provides judges with a wide-ranging and very flexible tool which allows them to look at all of the circumstances of a particular case in order to determine whether the restrictions on the worker's privacy were lawful.

B. Proportionality

Proportionality is another concept that is widely used as part of the judicial techniques that aim to reconcile privacy rights with workplace surveillance and the processing of workers' personal data. Indeed, because of the way that proportionality allows for a fair balance to be established between opposing interests and rights, it has been considered an essential element of any system of justice, at least since the days of Aristotle. Applying the concept, we can see that restrictions on the right to privacy may be accepted only insofar as

they are a proportionate response to a lawful aim pursued by the employer.

The concepts of proportionality and relevance are closely linked. While relevance requires that the means be related to the end, proportionality goes a step further by permitting judges to examine the suitability of those means for achieving that end. Relevance is thus a precondition for any assessment of proportionality (in that an action which is not relevant to a particular aim cannot be proportional); while proportionality means that it is not sufficient for an employer to show only that workplace surveillance or data processing is directly related to a legitimate aim of the company (and thus relevant), he or she must go on to show that the surveillance or data processing is not excessive with respect to that aim.

Proportionality will depend upon the assessment by a judge of whether a particular means was proportionate to a particular aim. Clearly, judges have a considerable margin of maneuver; and this in turn makes it rather difficult to establish general rules on which forms of surveillance and data processing are lawful, and which are not. Factors that may influence this decision may include the degree to which a particular case of surveillance was targeted (if there are problems in a particular department, surveillance of all the workforce may be a disproportionate response); and they may include the duration of the surveillance (if there are concerns over a specific spate of thefts within the company, the introduction of a permanent system of surveillance may similarly be disproportionate). In general, however, proportionality, as applied to surveillance and data processing, will be directly related to the restrictions that are imposed upon workers' privacy; the intensity and the scale of the restriction may be a part of this assessment, as may be the type of work done by the each individual worker (whether, for example, there is a greater or lesser need for the employer to ensure security).

III. THE ESTABLISHMENT OF PROCEDURAL RULES

The second type of regulatory technique that may be identified in this area is the establishment of procedural rules. Indeed, this seems to be part of a general increase in the use of this type of regulatory technique: imposing certain procedural requirements upon those whose actions may restrict the rights of other persons is a means of providing those other persons with certain guarantees; and, thus, to some extent, of establishing a balance between the conflicting rights, freedoms, and interests that may be involved. Specifically in the cases

of surveillance at work and the processing of workers' personal data, national laws establish two main sets of procedural rules: those which require the notification of the persons affected and those which require the notification of an independent authority. We shall look at each in turn.

A. The Notification of the Persons Affected

Requirements of notification may be established by judges, based, for example, on the general obligation to execute a contract in good faith. However, most national and international norms on workplace surveillance or data processing specifically require the prior notification of the subject; without it, these norms deem any such actions to be unlawful. Sometimes there are very specific legal requirements, such as that in Article L.121-8 of the French Labour Law Code, which stipulates that no information may be collected about employees or job candidates without their being informed beforehand. Much more general in its range are the requirements set out in Directive 95/46/EC, which apply to the collection of all personal data (and thus to almost all forms of surveillance at work): Article 10 establishes a list of procedural requirements which oblige data controllers to inform data subjects of the purposes of the processing, of the identity of the data controller and any representatives, and of any other facts that they must know in order for the processing to be fair to them. This last requirement gives judges considerable scope to adapt the requirements of notification to the particular case.

A further procedural requirement may be seen in the way that Articles 7 and 8 of the Directive place the consent of the data subject on the list of the circumstances in which data processing may be lawful (all data processing must fit into one of these circumstances and fulfill all the other conditions and requirements of the law). So, although the data subject's consent is certainly not always needed, an employer may sometimes be able to choose to follow this procedural rule in preference to seeking to justify data processing in relation to one of the other circumstances specified in the Directive. When an employer fulfills the procedural requirements with respect to notice and consent, this may then reduce the scope of employees' expectations and rights to privacy at work. The extent to which this may happen is an issue which is discussed elsewhere in this collection of papers.[3]

3. *See* Roberto Fragale Filho & Mark Jeffery, *Information Technology and Workers' Privacy: Notice and Consent*, 23 COMP LAB. L & POL'Y J. 551 (2002).

B. The Notification of an Independent Authority

Article 18 of Directive 95/46/EC requires data controllers to inform their national data protection authority of "any wholly or party automatic processing operation," which presumably includes all processing of personal data that involves a computer. This is an obligatory procedural requirement: as with other instances of the proceduralization of the law, if the relevant requirements are not followed, then the data processing will not be lawful; but, if they are followed, then employers will enjoy a certain assurance for the legitimacy of their actions. In this sense, the procedural requirements resemble substantive rules, as the fact that notification was or was not given—that is, whether the rules were or were not followed—will be the factor that determines the lawfulness or otherwise of an employer's actions.

This notification should then enable the national data protection authority to do its duties more effectively. Article 28 of the Directive requires all the Member States of the European Union to give certain supervisory powers on data protection to an independent public authority; and it also requires that these authorities be given wide-ranging powers and duties in order to protect and enforce the rights and freedoms of individual data subjects. This includes the power to investigate and intervene in specific cases, the power to engage in litigation, and the duty to hear claims from individual data subjects.

Far from being new, the creation of such independent authorities is a regulatory technique that has already been used in some of the Member States for a number of decades. Various authorities have been established in order to ensure the implementation of specific areas of law: they are often a practical means of reconciling conflicting rights and expectations, as well as economic and other interests. Such authorities may, like the data protection authorities, have the power to engage in litigation which seeks to enforce the legislation; and, indeed, their use as a regulatory technique may place the state in the curious position whereby one of these authorities may use its regulatory powers in order to limit the actions of another part of the state administration. In this way, this regulatory technique may blur the division between private and public law, something which has given rise to debates in civil law countries, especially with respect to the constitutional separation of powers.[4] Indeed, the use of the

4. *See* Claudia Faleri, *Information Technology and Workers' Privacy: Public and Private Regulation*, 23 COMP LAB. L & POL'Y J. 517 (2002); and specifically on the question of the

notification of state authorities as a regulatory technique may result in those authorities coming to appear as the regulatory authority in their specific area. (Remember that, in the case of the authorities created under Directive 95/46/EC, this area includes workplace surveillance as well as the processing of personal data about workers.) The use of this technique may then be linked to a more general trend whereby some areas of private law have been moved away from the usual processes of regulation. It appears that the government and the judiciary are to play a less important role in the development and enforcement of data protection than is the independent state authority.

IV. CONCLUSION

The regulatory techniques widely used with respect to workplace surveillance and the processing of workers' personal data are the establishment of general principles and the establishment of procedural rules. The establishment of general rules requires that a balance be set between workers' rights and expectations of privacy on the one hand, and employers' rights and expectations that they will be able to run their business on the other. (Both of these are recognized in the *European Charter of Fundamental Rights.*) This balance is often set using the concepts of relevance and proportionality. In this way, the use of general rules is a regulatory technique that allows judges to play an important part in the regulatory process. And, being a flexible technique, it has the advantage that it allows judges to adapt and change the nature of the balance according to the development of expectations and priorities within society as a whole. This may prove particularly important, giving the ever-greater importance that is being given to the idea of the rights of the individual.

The establishment of procedural rules is a less-flexible regulatory technique under which individual rights are protected through the establishment of procedural requirements that must be followed by those who wish to do things that would limit those individual rights. The law does not assess the behavior itself, but rather makes the lawfulness of the behavior conditional on the fulfillment of the procedural requirements. The purpose of procedures such as the notification of data processing to data subjects and national authorities is to promote data protection by allowing—and

separation of powers, *see* J. Chevallier, *Les Autorités Administratives Indépendantes et la Régulation des Marchés*, 1 REVUE JUSTICES 81 (1995).

encouraging—those individuals to exercise their rights, and those authorities to exercise their powers. The main risk is that the individuals may not have the strength, knowledge, or resources to act and that the national authorities become more concerned with the bureaucratic formality of notification itself than with the promotion of data protection in specific cases.[5]

5. Possibly for this reason, Directive 95/46/EC expressly requires Member States to allow data subjects access to the ordinary courts as well as to their national data protection authority.